EMBASSY SUITES®

San Francisco Airport - S San Francisco

February 7, 2014

Dear Guest:

On behalf of the San Francisco Airport – South San Francisco Embassy Suites hotel, I am writing to inform you about a recent incident involving two computers at the front desk of the hotel. We have learned that during the time of your stay at the San Francisco Airport – South San Francisco Embassy Suites hotel in 2013, an unauthorized third party obtained information relating to some payment cards used at the hotel. We have no evidence that your card was involved; however, we are sending you this notice out of an abundance of caution.

We began investigating the incident as soon as we learned of it and have determined that the incident involved a credit or debit card number, expiration date, cardholder name, and CVV2. Because the data was captured with a manual device, our computer systems were not breached and thus no other personal information about you or other guests was unlawfully obtained. We are working with law enforcement on the investigation of this incident and intend to prosecute the offenders. We have no reason to believe that this situation has impacted any other Embassy Suites hotel or any other hotel in our chain.

We recommend that you closely review the information included in this letter for some steps that you may take to protect yourself against any potential misuse of your payment card information.

I am truly sorry for any inconvenience this incident may have caused you. We greatly value your business and loyalty, and take this matter very seriously. As always, we will continue to work diligently to ensure that our guest information is protected.

Please contact us at **1-800-221-5031** if you have any questions.

Sincerely,

Rudy Ortiz
General Manager

EMBASSY SUITES®

San Francisco Airport - S San Francisco

U.S. State Notification Requirements

You should remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency and, if you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Under federal law, you are entitled to one free copy every 12 months of your credit report from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax (800) 525-6285 P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com	Experian (888) 397-3742 P.O. Box 9532 Allen, TX 75013 www.experian.com	TransUnion (800) 680-7289 Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790 www.transunion.com

In addition, you can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 (877) IDTHEFT (438-4338) http://www.ftc.gov/idtheft/	Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 (888) 743-0023 www.oag.state.md.us

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com